CLAIMS

What is claimed is:

1.   A method performed by a gaming system server, the method comprising:
        authenticating a gaming terminal;
        applying an encryption technique to encrypt a gaming software program, which
produces an encrypted gaming software program; and
        transmitting the encrypted gaming software program to the gaming terminal.

2.   The method of claim 1, further comprising:
        receiving a request to download the gaming software program from the gaming
terminal.

3.   The method of claim 1, wherein authenticating the gaming terminal comprises:
        receiving a gaming terminal digital certificate from the gaming terminal; and
        authenticating the gaming terminal based on the gaming terminal digital
certificate.

4.   The method of claim 1, further comprising:
        determining whether the gaming terminal is authorized to access the gaming
software program prior to transmitting the encrypted gaming software program.

5.   The method of claim 1, further comprising:
        generating a session key to use in applying the encryption technique.

6.   The method of claim 1, wherein the encryption technique is selected from a
group of encryption techniques that includes a symmetric encryption technique and an
asymmetric encryption technique.

7.   The method of claim 6, wherein the symmetric encryption technique is an encryption technique that uses a one-time session key.

8.   The method of claim 6, wherein the asymmetric encryption technique is selected from a group of asymmetric encryption techniques that includes a public key encryption technique, and a multiple-key public key encryption technique.

9.   The method of claim 1, further comprising:
       establishing a public-private key-pair, which includes a public key and a private key; and
       generating the gaming terminal digital certificate, which includes a digital certificate that is signed with the private key.

10.   A method performed by a gaming terminal, the method comprising:
       authenticating a gaming system server;
       receiving an encrypted gaming software program from the gaming system server; and
       applying a decryption technique to decrypt the encrypted gaming software program, which produces a gaming software program.

11.   The method of claim 10, further comprising:
       sending a request to download the gaming software program to the gaming system server.

12.   The method of claim 10, wherein authenticating the gaming system server comprises:
       receiving a gaming system server digital certificate from the gaming system server; and
       authenticating the gaming system server based on the gaming system server digital certificate.

13.   The method of claim 10, wherein the decryption technique is selected from a group of decryption techniques that includes a symmetric decryption technique and an asymmetric decryption technique.

14.   The method of claim 13, wherein the symmetric decryption technique is a decryption technique that uses a one-time session key.

15.   The method of claim 13, wherein the asymmetric decryption technique is selected from a group of asymmetric decryption techniques that includes a public key decryption technique, and a multiple-key public key decryption technique.

16.   The method of claim 10, further comprising:
      establishing a public-private key-pair, which includes a public key and a private key; and
      generating the gaming system server digital certificate, which includes a digital certificate that is signed with the private key.

17.   In a gaming system, a method comprising:
      a server of a gaming system generating a public-key private-key key pair;
      encrypting the public-key private-key key pair to produce an encrypted public-key private-key key pair;
      generating a certification authority digital certificate request, the certification authority digital certificate request including a public-key associated with the encrypted public-key private-key key pair;
      decrypting the public-key private-key key pair; and
      signing the certification authority digital certificate request using the private-key of the public-key private-key key pair to form the certification authority digital certificate.

18.   In a gaming system, a method comprising:
      a server of a gaming system generating a public-key private-key key pair;

generating an unsigned digital certificate request, the unsigned digital certificate request including the public-key associated with the encrypted public-key private-key key pair;

providing the unsigned digital certificate request to an approval authority; and

receiving, from the approval authority, a signed digital certificate associated with the unsigned digital certificate request, the signed digital certificate including a digital signature from the approval authority, the digital signature formed by digitally signing the public-key of the public-key private-key key pair with an approval authority private-key from an approval authority public-key private-key key pair, the digital signature linking the signed digital certificate to the approval authority.

19.   In a gaming system, a method comprising:

a server of a gaming system generating a public-key private-key key pair;

generating an unsigned digital certificate request, the unsigned digital certificate request including the public-key associated with the encrypted public-key private-key key pair;

providing the unsigned digital certificate request to an approval authority; and

receiving, from the approval authority, a signed digital certificate associated with the unsigned digital certificate request, the signed digital certificate including a digital signature from the approval authority, the digital signature formed by digitally signing the public-key of the public-key private-key key pair with an approval authority private-key from an approval authority public-key private-key key pair, the digital signature linking the signed digital certificate to the approval authority.

20.   In a gaming system, a method comprising:

receiving a first signed digital certificate from a server, the first signed digital having an associated first public-key private-key key pair and having a first digital signature from an approval authority, the first digital signature formed by digitally signing the first public-key of the first public-key private-key key pair with a first approval authority private-key from a first approval authority public-key private-key key pair;

authenticating the server based on the first signed digital certificate;

creating a premaster secret based on the first signed digital certificate;

encrypting the premaster secret with the first public-key of the first public-key private-key key pair to form an encrypted premaster secret;

transmitting the encrypted premaster secret to the server;

transmitting a second signed digital certificate, the second signed digital certificate including a second public key of an associated second public-key private-key key pair and a second digital signature, the second digital signature formed by digitally signing the second public-key of the associated second public-key private-key key pair with a second approval authority private-key from a second approval authority public-key private-key key pair;

transmitting digitally signed random data, the digitally signed random data comprising randomly generated data and a third digital signature, the third digital signature formed by encrypting a one-way hash with the second private-key of the associated second public-key private-key key pair, the one-way hash formed from the randomly generated data;

receiving a master secret, the master secret formed by decrypting the encrypted premaster secret with the first private-key of the first public-key private-key key pair;

generating a session key from the master secret;

transmitting a first message to the server, the first message indicating a session key use;

receiving a second message from the server, the second message indicating the session key use; and

receiving session key encrypted data based on an access control list, the access control list comprising the access information.

21. In a gaming system, a method comprising:

receiving a signed digital certificate from a server, the signed digital certificate having an associated public-key private-key key pair and having a digital signature from an approval authority, the digital signature formed by digitally signing the public-key of

the public-key private-key key pair with an approval authority private-key from an approval authority public-key private-key key pair;

verifying a validity period of the digital certificate;

validating the digital signature of the signed digital certificate if the period of the digital certificate is valid;

validating a location of the server if the digital signature of the signed digital certificate is valid; and

authenticating the server if the location of the server is valid.

22.   In a gaming system, a method comprising:

receiving a signed digital certificate from a gaming terminal, the signed digital certificate including a public key of an associated public-key private-key key pair and a first digital signature from an approval authority, the first digital signature formed by digitally signing the public-key of the associated public-key private-key key pair with an approval authority private-key from an approval authority public-key private-key key pair;

receiving digitally signed random data from the gaming terminal, the digitally signed random data comprising randomly generated data and a second digital signature, the second digital signature formed by encrypting a one-way hash with the private-key of the associated public-key private-key key pair, the one-way hash formed from the randomly generated data;

validating the second digital signature with the public-key of the associated public-key private-key key pair to authenticate the gaming terminal;

verifying a validity period of the signed digital certificate if the second digital signature is valid;

validating an approval authority associated with the first digital signature if the period of the digital certificate is valid;

validating the first digital signature if the approval authority is valid; and

enabling the gaming terminal to receive data based on an access control list, the access control list comprising the gaming terminal access information.

23.   A gaming system comprising:

one or more gaming system servers, wherein selected ones of the one or more gaming system servers authenticate a gaming terminal, apply an encryption technique to encrypt a gaming software program, which produces an encrypted gaming software program, and transmit the encrypted gaming software program to the gaming terminal; and

one or more gaming terminals, wherein selected ones of the one or more gaming terminals authenticate a gaming system server, receive the encrypted gaming software program from the gaming system server, and apply a decryption technique to decrypt the encrypted gaming software program, which produces the gaming software program.

24.   A computer-readable medium having program instructions stored thereon to perform a method, which when executed within an electronic device, result in:

a gaming system server authenticating a gaming terminal;

applying an encryption technique to encrypt a gaming software program, which produces an encrypted gaming software program; and

transmitting the encrypted gaming software program to the gaming terminal.

25.   A computer-readable medium having program instructions stored thereon to perform a method, which when executed within an electronic device, result in:

a gaming terminal authenticating a gaming system server;

receiving an encrypted gaming software program from the gaming system server; and

applying a decryption technique to decrypt the encrypted gaming software program, which produces a gaming software program.